3.05 Policy

Privacy and Confidentiality

Policy Statement
Burke and Beyond is committed to protecting the privacy and confidentiality of participants, their families, staff and community partners who associate with us. Protecting personal information is paramount to develop and maintain relationships and ensure our business success.

In accordance with the "Enhancing Privacy Protection" Act 2012, Privacy Act 2000 and Health Records Act 2001 Burke and Beyond is committed to protecting the privacy of personal information which is requested and handled on behalf of the participants and employees. Burke and Beyond respect an individual's right to privacy, and any personal information provided by the participants and staff to the organisation will be held in confidence.

Objective
Our respect for the right to privacy and confidentiality of personal information is paramount. We have policies and procedures to ensure that all personal information, no matter how or where it is obtained, is handled sensitively, securely, and in accordance with the relevant legislation and standards.
We only collect such information for lawful purposes and as is reasonably necessary. We will ensure reasonable steps are taken to secure personal information from misuse, loss or unauthorised access, modification or disclosure.
It is the aim of Burke and Beyond to ensure all people are afforded the opportunity to provide informed consent for the sharing and/or use of personal information and images.

Scope
This policy applies to all staff, volunteers, participants, their families and business/community partners who collect, receive and/or have access to personal information about participants and staff.

Definitions:

Privacy	The freedom from intrusion into one's personal matters, and personal information.
Confidentiality	Personal information shared with an official person (attorney, physician, therapist, paid support), or an organisation, which cannot be divulged to another party without express consent of the individual.

Collection of Information
Burke and Beyond collect and handle a range of personal information for the purposes of providing services, managing staff or carrying out a statutory function. We also collect some personal information for planning, funding, monitoring, and evaluation of services and functions, however where practicable we will remove identifying details for these purposes. The information will otherwise be restricted to program use and organisational management, unless requested for legal purposes. There are very few situations when information can be shared without obtaining consent. For example, in an emergency, we would need to release medical or personal information to aid emergency treatment.
Also in certain circumstances, this organisation may be required by law to release personal information.

Examples include:
- Reporting of notifiable diseases to the Department of Health and Human Services.
- Providing health records to a court when required in relation to legal proceedings.
- Providing health records to a law enforcement agency in response to a search warrant.

If any of these circumstances apply, Burke and Beyond will advise the person as soon as possible and where appropriate that their information has been released and the purpose of its release.
Burke and Beyond will only collect information which is necessary for us to provide an effective and appropriate service. We will ensure the consent of participants, their carers and staff if we collect information relating to them from other sources. Consent will be obtained to use this information for any other purpose.

Data Quality
We endeavor at all times to ensure information collected by the organisation about participants, staff or volunteers is accurate and up to date. We encourage individuals and carers to notify us of any inaccurate information so that it can be updated or corrected.

Access to personal information
The participant or their authorised representative, and staff of the organisation may review their personal information or file held by Burke and Beyond by writing a letter to the CEO requesting access.

Security of personal information
At Burke and Beyond, we make every effort to see that personal information remains secure and protected from unauthorised or miss- appropriate access. Information or data is restricted to those who need to know, with the distribution of such information kept to a minimum.

Participant information
Participant information not required for daily support is housed on the client management system and scanned and uploaded as needed to our database. Hard copies are kept in a locked filing cabinet in rooms or in our archives. All personal day to day information on participants attending Burke and Beyond is held securely under lock and key. Only staff members who work with participants and their managers have access.

Sensitive Information
We will not collect any sensitive information about participants except were directed to for a specific purpose or required for support planning. Sensitive information is generally regarded as information relating to things such as: diversity, religion, culture, political viewpoints, sexuality and criminal records. As part of the Commonwealth Minimum Data Set conducted annually, a requirement to report a person's ethnic background is requested. Other identifiers are not used such as names, phone numbers and addresses.

Openness
Burke and Beyond is completely open with what we do with personal information as shown by:

- the contents of this Policy;
- privacy statements included in correspondence of a personal nature to participants, carers and community partners;
- Personal Data Management System implemented.

Disposal and Retention
Burke and Beyond will retain and dispose of documents and electronic records in line with Public Record Office *"PROS 08/13 Retention and Disposal authority for the Records of the Disability Services Function".* Confidential documents in hard copy will be disposed of through a suitable contractor using locked recycling bins.

Breaches of this policy
The organisation will ensure that all staff, participants and members of the Board are aware of the details contained in this policy and that personal information is kept in strict confidence and securely stored.
In the first instance, alleged breaches of privacy and confidentiality should be referred to the CEO.

If a satisfactory resolution cannot be reached through the feedback and complaints processes, the CEO will report the allegation to the Board of Management and consult with the Health Services Commission to seek advice. If a person is not satisfied with the way Burke and Beyond handle the allegation they may take further action.

There is a formal legal requirement to provide notice of any serious breaches to an affected individual/s and the Privacy Commissioner should a serious breach be identified.
At Burke and Beyond, we store personal information and have strict obligations under the Privacy Act not to disclose it to third parties otherwise than in accordance with the Act. If there is a breach caused by employee error, system glitch, third party theft or cyber-attack, this breach may need to be reported.

In order to determine whether a privacy breach requires notification, the reviewing person would need to conclude there has been unauthorised access to, unauthorised disclosure of, or loss of, personal information held by Burke and Beyond, and that this would likely result in serious harm being caused to any of the individuals to whom the information relates. Serious harm could include physical, psychological, emotional, economic, financial and reputation harm.
Not all data breaches will require notifications.
In determining the seriousness of the breach Burke and Beyond will review the type of information leaked, the sensitivity of the information, the kind of persons who may have obtained the information, and whether the information has been otherwise protected. Information likely to give rise to the risk of harm, including, but not limited to, things like credit card or account details, medical information, personal contact details.

1. If staff believe there are reasonable grounds to suspect there may have been an eligible privacy/ data breach, report and discuss with your immediate manager/ coordinator
2. Your manager/ coordinator will report it to the CEO as soon as practicable.
3. The CEO will discuss/ review details and/ or:
    a. Acknowledge, confirm breach and determine level of seriousness
    b. As relevant, report to the Privacy Commissioner as soon as practicable
    c. Maintain a register for breaches
    d. Initiate an investigation into the breach and provide outcome report to Privacy Commissioner within 30 days
    e. Inform and discuss with individual/s affected

Provide report to Board of Management

Fines for breaches of the Act can be significant. Failure to comply with the requirement to notify will be deemed to be a serious interference with the privacy of an individual and may incur a fine of:

- Up to $420,000 for an individual
- Up to $2.1 million for a body corporate

Implementation and Review
This document will be reviewed every three years and following significant incidents if they occur. Improvements to this document can be made by completing a suggestion and improvement form, attaching any suggested amendments and forwarding to your manager and/or the Manager Quality and Risk review.

Administration:

Standards related to:	Rights and Responsibilities – Privacy and Dignity
Legislation or external reference documents*:*	National Standards for Disability Services National Standards for Disability Services | Department of Social Services, Australian Government (dss.gov.au) Privacy Act (1988) (Commonwealth) Enhancing Privacy Protection" Act 2012, Information Privacy Act 2000 (State)

	Health Records Act 2001	
Related Policies or Procedures*:*	Code of Conduct Information and Communication Technology Policy Service Access Procedure Consent Policy Auditing and Document Control Records Management Policy and Procedure	
Reviewing and approving this policy		
Frequency	**Person responsible**	**Approval**
Every 3 years	Manager Quality and Risk	CEO

Indexing:

Policy review and version tracking			
Review	**Date Approved**	**Approved by**	**Next Review Due**
1	21/09/2020	Bruno Cyr	2023
2	16/05/2024	Lisa Sawatzky	2025